PIX/ASA 7.x: Abilita/Disabilita la comunicazione tra le interfacce

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per diverse forme di comunicazione tra le interfacce sull'appliance di sicurezza ASA/PIX.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Assegnazione indirizzi IP e gateway predefinito
- Connettività di rete fisica tra dispositivi
- Numero porta di comunicazione identificato per il servizio implementato

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Adaptive Security Appliance con software versione 7.x e successive
- Server Windows 2003
- Workstation Windows XP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con le seguenti versioni hardware e software:

- PIX serie 500 firewall con versione 7.x e successive

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

In questo documento viene descritta la procedura da seguire per permettere la comunicazione tra diverse interfacce. Le forme di comunicazione come queste sono discusse:

1. Comunicazioni da host situati all'esterno che richiedono l'accesso alle risorse situate nella zona demilitarizzata
2. Comunicazione dagli host della rete interna che richiedono l'accesso alle risorse presenti nella DMZ
3. Comunicazione dagli host all'interno e dalla rete DMZ che richiedono l'accesso alle risorse all'esterno

NAT

Nell'esempio, vengono utilizzati Network Address Translation (NAT) e Port Address Translation (PAT) nella configurazione. La conversione degli indirizzi sostituisce l'indirizzo reale (locale) in un pacchetto con un indirizzo mappato (globale) instradabile sulla rete di destinazione. NAT è costituito da due passaggi: processo in cui un indirizzo reale viene convertito in un indirizzo mappato e quindi il processo di annullamento della traduzione per il traffico che restituisce. In questa guida alla configurazione sono disponibili due forme di traduzione degli indirizzi: Statico e dinamico.

Le traduzioni dinamiche consentono a ciascun host di utilizzare un indirizzo o una porta diversi per ciascuna traduzione successiva. Le traduzioni dinamiche possono essere utilizzate quando gli host locali condividono o "nascondono" uno o più indirizzi globali comuni. In questa modalità un indirizzo locale non può riservare in modo permanente un indirizzo globale per la traduzione. Al contrario, la traduzione degli indirizzi avviene su base molti a uno o molti a molti e le voci di

traduzione vengono create solo quando sono necessarie. Non appena una voce di traduzione è libera da utilizzare, viene eliminata e resa disponibile agli altri host locali. Questo tipo di conversione è particolarmente utile per le connessioni in uscita, in cui agli host interni viene assegnato un indirizzo dinamico o un numero di porta solo quando vengono stabilite connessioni. Esistono due forme di traduzione dell'indirizzo dinamico:

- NAT dinamico - Gli indirizzi locali vengono convertiti nel successivo indirizzo globale disponibile in un pool. Poiché la traduzione viene eseguita singolarmente, è possibile esaurire il pool di indirizzi globali nel caso in cui un numero maggiore di host locali richieda la traduzione in un determinato momento.
- NAT Overload (PAT) - Gli indirizzi locali vengono convertiti in un unico indirizzo globale; ogni connessione viene resa univoca quando il successivo numero di porta di ordine superiore disponibile dell'indirizzo globale viene assegnato come origine della connessione. La traduzione viene eseguita su base molti a uno perché molti host locali condividono un unico indirizzo globale.

La traduzione statica crea una traduzione fissa degli indirizzi reali negli indirizzi mappati. Una configurazione NAT statica mappa lo stesso indirizzo per ogni connessione da parte di un host ed è una regola di conversione persistente. Le traduzioni degli indirizzi statici vengono utilizzate quando un host interno o locale deve disporre dello stesso indirizzo globale per ogni connessione. La traduzione degli indirizzi viene eseguita singolarmente. Le traduzioni statiche possono essere definite per un singolo host o per tutti gli indirizzi contenuti in una subnet IP.

La differenza principale tra NAT dinamico e un intervallo di indirizzi per NAT statico è che NAT statico consente a un host remoto di avviare una connessione a un host tradotto (se esiste un elenco degli accessi che lo consente), a differenza di NAT dinamico. È inoltre necessario un numero uguale di indirizzi mappati con NAT statico.

L'appliance di sicurezza converte un indirizzo quando una regola NAT corrisponde al traffico. Se nessuna regola NAT corrisponde, l'elaborazione del pacchetto continua. L'eccezione si verifica quando si abilita il controllo NAT. Il controllo NAT richiede che i pacchetti che attraversano da un'interfaccia di sicurezza superiore (interna) a un livello di sicurezza inferiore (esterna) corrispondano a una regola NAT, altrimenti l'elaborazione del pacchetto viene interrotta. Per visualizzare informazioni di configurazione comuni, consultare il documento PIX/ASA 7.x NAT and PAT. Per una comprensione più approfondita del funzionamento di NAT, fare riferimento alla guida sul funzionamento di NAT.

Suggerimento: ogni volta che si modifica la configurazione NAT, si consiglia di cancellare le traduzioni NAT correnti. Potete cancellare la tabella di traslazione con il comando **cancella (clear xlate)**. **Tuttavia, è necessario prestare attenzione quando si esegue questa operazione,** poiché se si cancella la tabella di conversione vengono disconnesse tutte le connessioni correnti che utilizzano le traduzioni. L'alternativa alla cancellazione della tabella di conversione consiste nell'attendere il timeout delle traduzioni correnti, ma questa opzione non è consigliata in quanto la creazione di nuove connessioni con le nuove regole può causare un comportamento imprevisto.

Livelli di protezione

Il valore del livello di protezione controlla il modo in cui gli host e i dispositivi sulle diverse interfacce interagiscono tra loro. Per impostazione predefinita, gli host e i dispositivi connessi alle interfacce con livelli di protezione più elevati possono accedere agli host e ai dispositivi connessi alle interfacce con livelli di protezione più bassi. Gli host/dispositivi connessi alle interfacce con interfacce con sicurezza inferiore non possono accedere agli host/dispositivi connessi alle

interfacce con interfacce con sicurezza superiore senza l'autorizzazione di elenchi degli accessi.

Il comando **security-level** è una novità della versione 7.0 e sostituisce la parte del comando **nameif** che ha assegnato il livello di protezione per un'interfaccia. Due interfacce, "l'interno" e "l'esterno", hanno livelli di sicurezza predefiniti, ma possono essere sostituiti con il comando **security-level**. Se all'interfaccia viene assegnato il nome "inside", il livello di protezione predefinito è 100; a un'interfaccia denominata "external" viene assegnato un livello di protezione predefinito pari a 0. A tutte le altre interfacce appena aggiunte viene assegnato un livello di protezione predefinito pari a 0. Per assegnare un nuovo livello di protezione a un'interfaccia, utilizzare il comando **security-level** in modalità di comando dell'interfaccia. I livelli di protezione sono compresi tra 1 e 100.

Nota: i livelli di protezione vengono utilizzati solo per determinare il modo in cui il firewall controlla e gestisce il traffico. Ad esempio, il traffico che passa da un'interfaccia con un livello di sicurezza più elevato a una più bassa viene inoltrato con criteri predefiniti meno rigidi rispetto al traffico che arriva da un'interfaccia con un livello di sicurezza più basso a una con un livello di sicurezza più alto. Per ulteriori informazioni sui livelli di sicurezza, consultare la guida di riferimento dei comandi ASA/PIX 7.x.

ASA/PIX 7.x ha anche introdotto la possibilità di configurare più interfacce con lo stesso livello di sicurezza. Ad esempio, è possibile assegnare a più interfacce collegate a partner o ad altre DMZ il livello di protezione 50. Per impostazione predefinita, queste stesse interfacce di protezione non possono comunicare tra loro. Per ovviare a questo problema, è stato introdotto il comando **inter-interface-**security-traffic-allowed. Questo comando consente la comunicazione tra interfacce con lo stesso livello di protezione. Per ulteriori informazioni sulla stessa sicurezza tra le interfacce, consultare la guida di riferimento ai comandi Configurazione dei parametri di interfaccia e questo esempio.

ACL

Gli elenchi di controllo di accesso sono in genere composti da più voci di controllo di accesso (ACE, Access Control Entry) organizzate internamente da Appliance di sicurezza in un elenco collegato. Le voci di controllo di accesso descrivono un insieme di traffico, ad esempio quello proveniente da un host o da una rete, e elencano un'azione da applicare al traffico, in genere consentita o negata. Quando un pacchetto è soggetto al controllo dell'elenco degli accessi, Cisco Security Appliance cerca in questo elenco collegato di ACE per trovarne uno che corrisponda al pacchetto. **La prima voce ACE corrispondente all'appliance di sicurezza è quella applicata al pacchetto.** Una volta trovata la corrispondenza, l'azione in tale voce (autorizzazione o rifiuto) viene applicata al pacchetto.

Èconsentito un solo elenco degli accessi per interfaccia, per direzione. Ciò significa che è possibile avere un solo elenco degli accessi relativo al traffico in entrata su un'interfaccia e un solo elenco degli accessi relativo al traffico in uscita su un'interfaccia. Gli elenchi degli accessi che non vengono applicati alle interfacce, ad esempio gli ACL NAT, sono illimitati.

Nota: per impostazione predefinita, tutti gli elenchi degli accessi hanno alla fine un'ACE implicita che nega tutto il traffico, quindi tutto il traffico che non corrisponde ad alcuna ACE immessa nell'elenco degli accessi corrisponde all'ultimo rifiuto implicito e viene scartato. Per consentire il flusso del traffico, è necessario disporre di almeno un'istruzione di autorizzazione in un elenco di accesso di interfaccia. Senza un'autorizzazione, tutto il traffico viene rifiutato.

Nota: l'elenco degli accessi viene implementato con i comandi **access-list** e **access-group**. Questi comandi vengono utilizzati al posto dei comandi **conduit** e **outbound**, utilizzati nelle versioni

precedenti del software PIX firewall. Per ulteriori informazioni sugli ACL, consultare il documento sulla configurazione dell'elenco degli accessi IP.

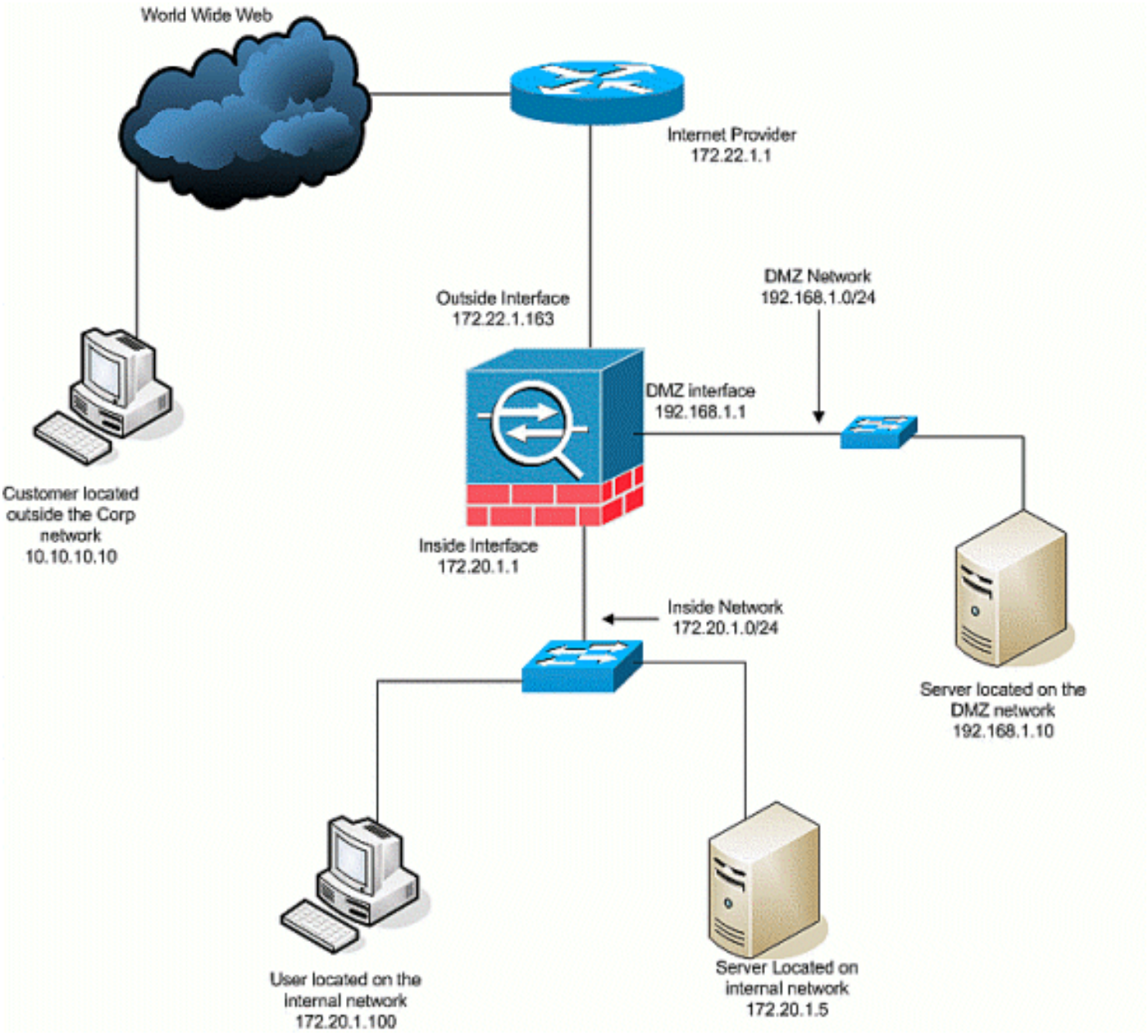
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata la seguente impostazione di rete:



Configurazione iniziale

Nel documento vengono usate queste configurazioni:

- Con questa configurazione di base del firewall, non sono attualmente disponibili istruzioni NAT/STATIC.
- Non sono stati applicati ACL, quindi è in uso l'ACE implicito `deny any`.

Nome dispositivo 1

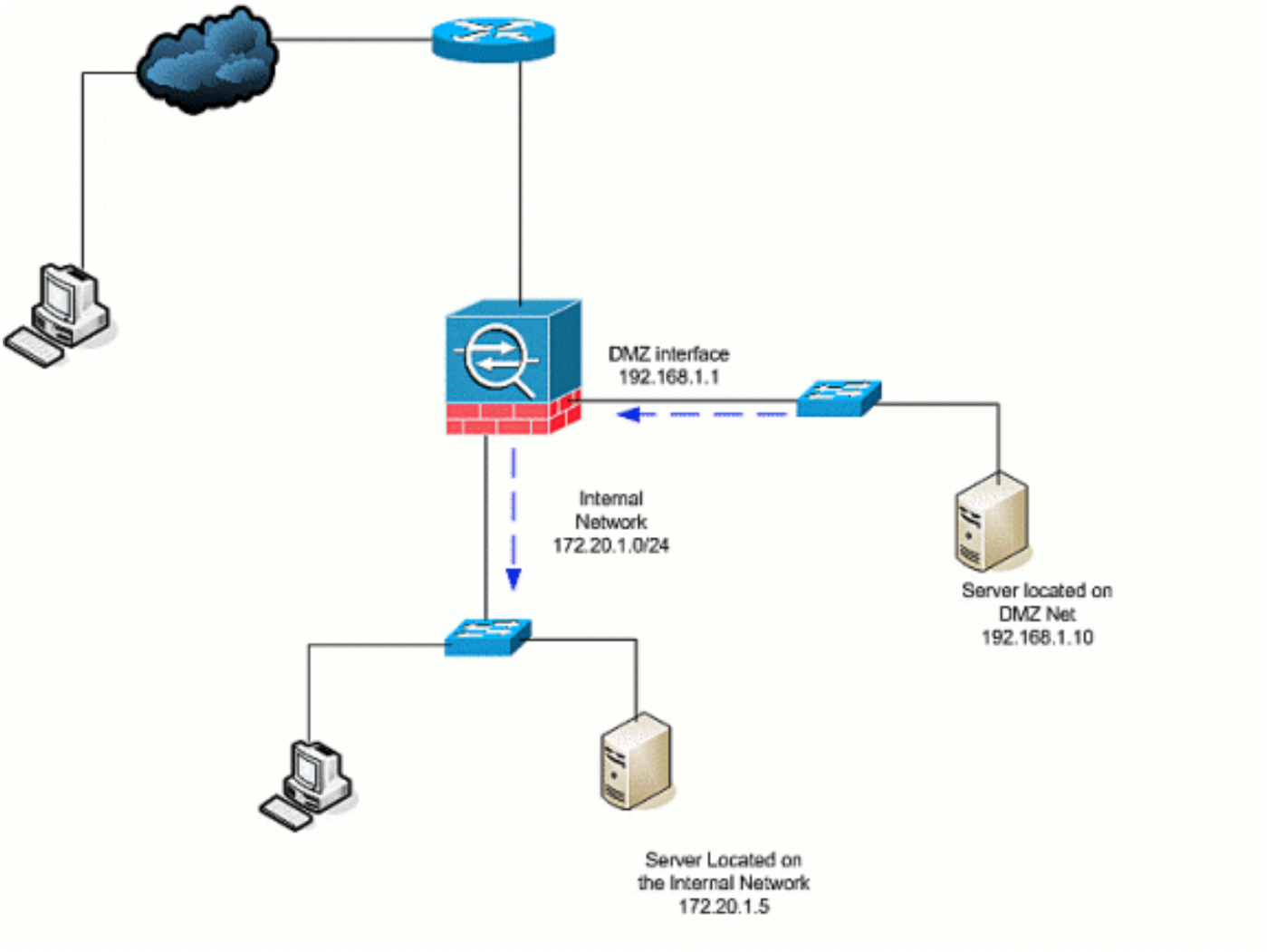
```
ASA-AIP-CLI(config)#show running-config

 ASA Version 7.2(2)
!
hostname ASA-AIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 172.22.1.163 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.20.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 50
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/3
 nameif DMZ-2-testing
 security-level 50
 ip address 192.168.10.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu inside 1500
mtu Outside 1500
mtu DMZ 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat-control
route Outside 0.0.0.0 0.0.0.0 172.22.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
```

```
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA-AIP-CLI(config)#
```

DMZ verso l'interno

Per consentire la comunicazione dalla DMZ agli host della rete interna, utilizzare questi comandi. In questo esempio, un server Web nella DMZ deve accedere a un server AD e DNS nella parte interna.

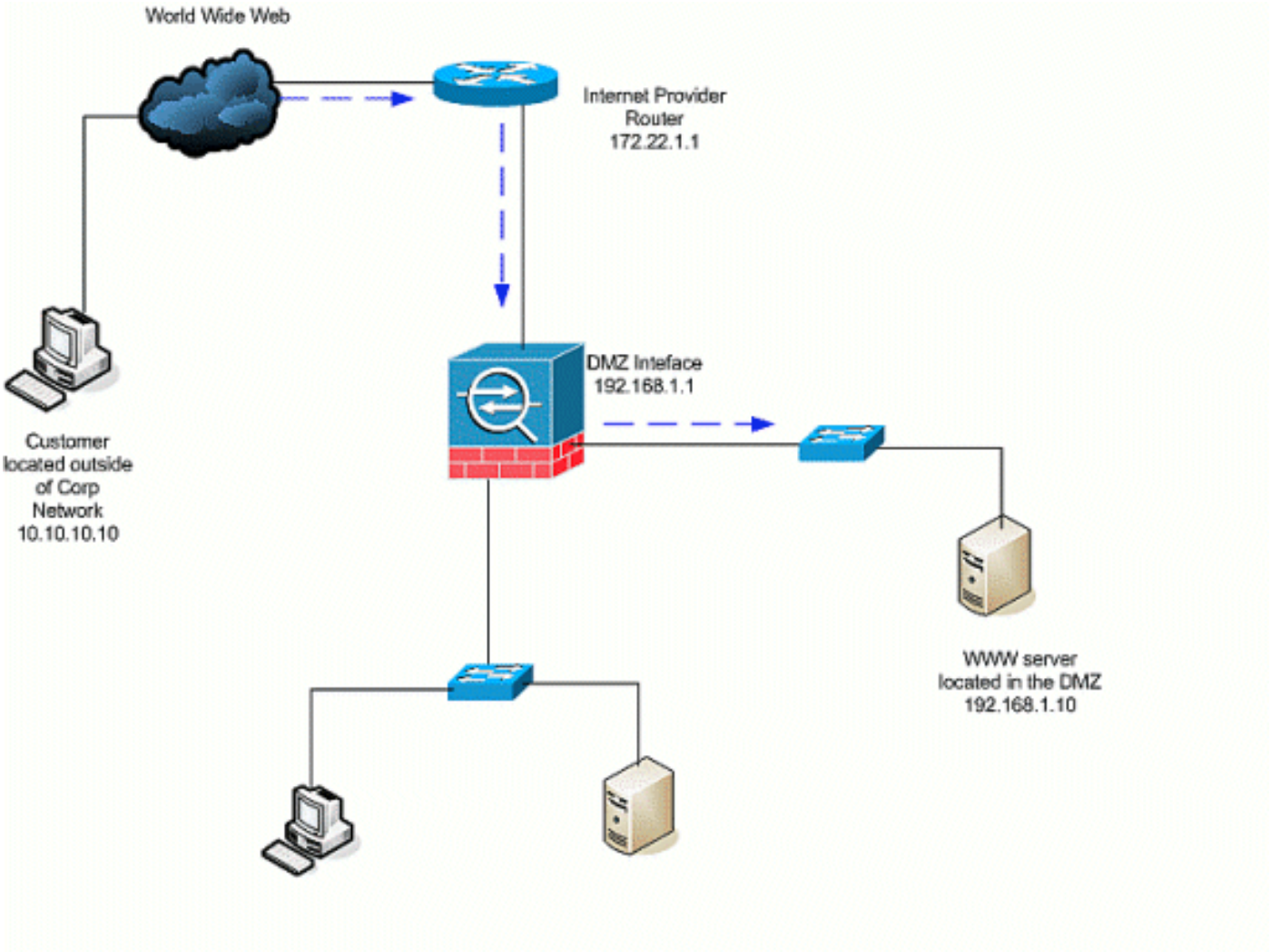


1. Creare una voce NAT statica per il server AD/DNS nella DMZ. NAT statico crea una traduzione fissa di un indirizzo reale in un indirizzo mappato. Questo indirizzo mappato è un indirizzo che gli host DMZ possono utilizzare per accedere al server all'interno senza dover conoscere l'indirizzo reale del server. Questo comando mappa l'indirizzo DMZ 192.168.2.20 all'indirizzo interno reale 172.20.1.5.`ASA-AIP-CLI(config)# static (inside,DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255`
2. Gli ACL sono necessari per consentire a un'interfaccia con un livello di sicurezza inferiore di accedere a un livello di sicurezza superiore. In questo esempio, al server Web che si trova nella zona DMZ (Security 50) viene concesso l'accesso al server AD/DNS nella zona interna (Security 100) con queste porte di servizio specifiche: DNS, Kerberos e LDAP.`ASA-AIP-CLI(config)# access-list DMZtoInside extended permission udp host 192.168.1.10 host 192.168.2.20 eq domainASA-AIP-CLI(config)# access-list DMZtoInside extended allow tcp host 192.168.1.10 host 192.168.2.20 eq 88ASA-AIP-CLI(config)# access-list DMZtoInside extended permission udp host 192.168.1.10 host 192.168.2.20 eq 389`**Nota:** gli ACL consentono l'accesso all'indirizzo mappato del server AD/DNS creato in questo esempio e non all'indirizzo interno reale.
3. In questo passaggio verrà applicato l'ACL all'interfaccia DMZ nella direzione in entrata con questo comando:`ASA-AIP-CLI(config)# access-group DMZtoInside nella DMZ dell'interfaccia`**Nota:** se si desidera bloccare o disabilitare la porta 88, ad esempio, il traffico dalla DMZ all'interno, utilizzare questo:
   ```
   ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit
   tcp host 192.168.1.10 host 192.168.2.20 eq 88
   ```
   Suggerimento: ogni volta che si modifica la configurazione NAT, si consiglia di cancellare le traduzioni NAT correnti. Potete cancellare la tabella di traslazione con il comando **cancella**

(clear xlate). **Prestare attenzione quando si esegue questa operazione** poiché la cancellazione della tabella di conversione determina la disconnessione di tutte le connessioni correnti che utilizzano le traduzioni. L'alternativa alla cancellazione della tabella di conversione consiste nell'attendere il timeout delle traduzioni correnti, ma questa opzione non è consigliata in quanto la creazione di nuove connessioni con le nuove regole può causare un comportamento imprevisto.Altre configurazioni comuni sono:Server di posta nella DMZAccesso SSH interno ed esternoSessioni di desktop remoto consentite tramite dispositivi PIX/ASAAltre soluzioni DNS se utilizzate nella DMZ

Internet su DMZ

Per consentire le comunicazioni tra utenti su Internet o tramite l'interfaccia esterna (Protezione 0) e un server Web nella zona DMZ (Protezione 50), utilizzare i seguenti comandi:



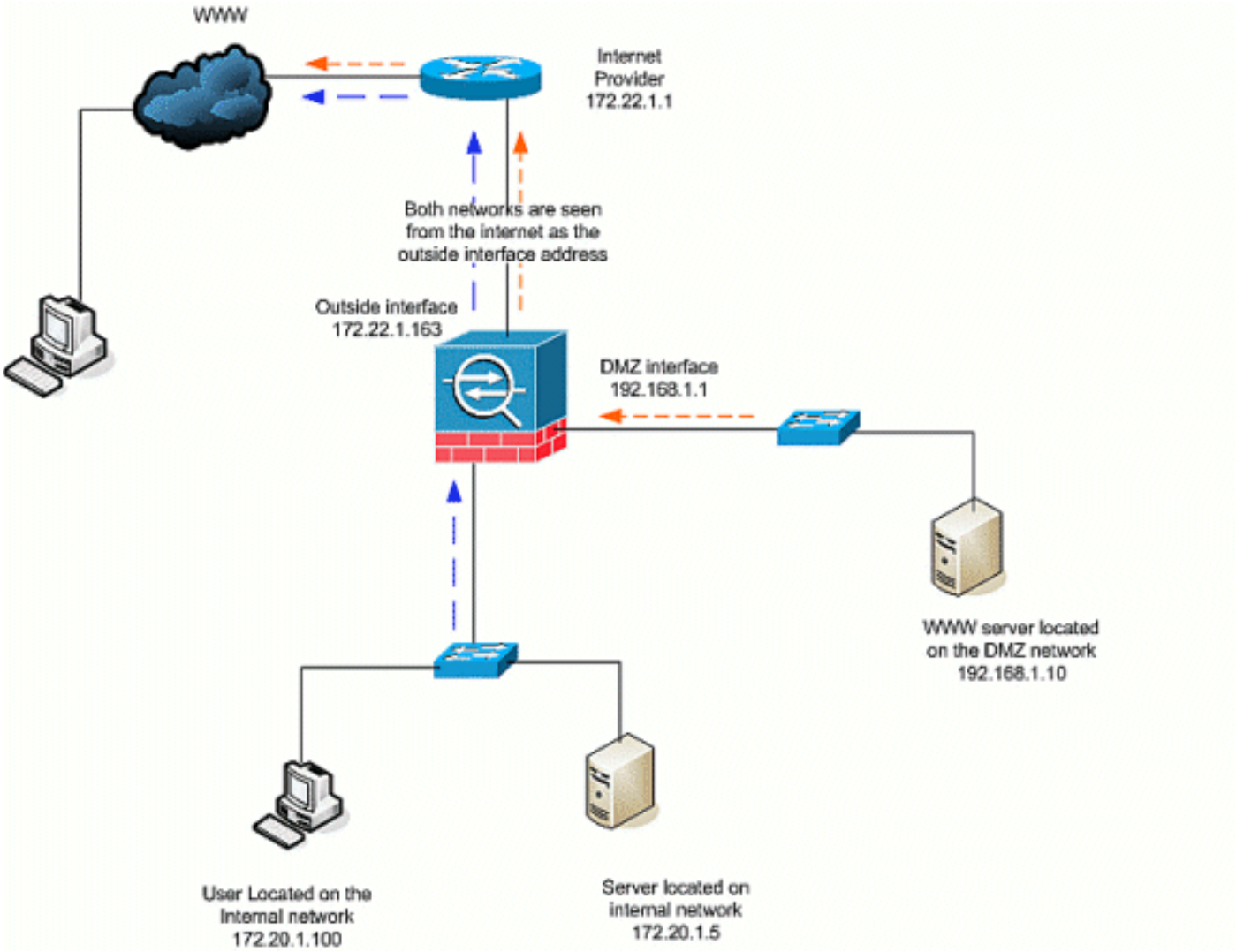
1. Creare una traduzione statica verso l'esterno per il server Web nella DMZ. NAT statico crea una traduzione fissa di un indirizzo reale in un indirizzo mappato. Questo indirizzo mappato è un indirizzo che gli host su Internet possono utilizzare per accedere al server Web sulla DMZ senza dover conoscere l'indirizzo reale del server. Questo comando mappa l'indirizzo esterno 172.22.1.25 all'indirizzo DMZ reale 192.168.1.10.`ASA-AIP-CLI(config)# static (DMZ,Outside) 172.22.1.25 192.168.1.10 netmask 255.255.255.255`
2. Creare un ACL che consenta agli utenti esterni di accedere al server Web tramite l'indirizzo mappato. Il server Web ospita anche l'FTP.`ASA-AIP-CLI(config)# access-list Al di fuori di DMZ extended allow tcp any host 172.22.1.25 eq wwwASA-AIP-CLI(config)# access-list Al di`

```
fuori di DMZ extended allow tcp any host 172.22.1.25 eq ftp
```

3. L'ultimo passaggio della configurazione è applicare l'ACL all'interfaccia esterna per il traffico in direzione in entrata.`ASA-AIP-CLI(config)# access-group esterno a DMZ nell'interfaccia esterna`**Nota:** è possibile applicare un solo elenco degli accessi per interfaccia e per direzione. Se all'interfaccia esterna è già stato applicato un ACL in entrata, non è possibile applicare questo ACL di esempio. Aggiungere invece le voci ACE dell'esempio nell'ACL corrente applicato all'interfaccia.**Nota:** per bloccare o disabilitare il traffico FTP da Internet a DMZ, ad esempio, utilizzare questo:
```
ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit
tcp any host 172.22.1.25 eq ftp
```
Suggerimento: ogni volta che si modifica la configurazione NAT, si consiglia di cancellare le traduzioni NAT correnti. Potete cancellare la tabella di traslazione con il comando **cancella (clear xlate)**. **Prestare attenzione quando si esegue questa operazione** poiché la cancellazione della tabella di conversione determina la disconnessione di tutte le connessioni correnti che utilizzano le traduzioni. L'alternativa alla cancellazione della tabella di conversione consiste nell'attendere il timeout delle traduzioni correnti, ma questa opzione non è consigliata in quanto la creazione di nuove connessioni con le nuove regole può causare un comportamento imprevisto.

DMZ a Internet

In questo scenario, gli host posizionati sull'interfaccia interna (Security 100) dell'accessorio di protezione potranno accedere a Internet dall'interfaccia esterna (Security 0). Ciò si ottiene con il PAT, o sovraccarico NAT, forma di NAT dinamico. A differenza degli altri scenari, in questo caso non è necessario un ACL perché gli host su un'interfaccia di sicurezza elevata accedono agli host su un'interfaccia di sicurezza bassa.



1. Specificare le origini del traffico da convertire. In questo caso è definita la regola NAT numero **1** e tutto il traffico proveniente dall'interno e dagli host DMZ è consentito.`ASA-AIP-CLI(config)# nat (inside) 1 172.20.1.0 255.255.255.0ASA-AIP-CLI(config)# nat (inside) 1 192.168.1.0 255.255.255.0`
2. Specificare l'indirizzo, il pool di indirizzi o l'interfaccia che il traffico NAT deve utilizzare quando accede all'interfaccia esterna. In questo caso, il comando PAT viene eseguito con l'indirizzo dell'interfaccia esterna. Questa funzione è particolarmente utile quando l'indirizzo dell'interfaccia esterna non è noto in precedenza, ad esempio in una configurazione DHCP. In questo caso, il comando globale viene emesso con lo stesso ID NAT **1**, che lo lega alle regole NAT dello stesso ID.`Interfaccia globale ASA-AIP-CLI(config)# (esterna) 1`

Suggerimento: ogni volta che si modifica la configurazione NAT, si consiglia di cancellare le traduzioni NAT correnti. Potete cancellare la tabella di traslazione con il comando **cancella (clear xlate)**. **Prestare attenzione quando si esegue questa operazione** poiché la cancellazione della tabella di conversione determina la disconnessione di tutte le connessioni correnti che utilizzano le traduzioni. L'alternativa alla cancellazione della tabella di conversione consiste nell'attendere il timeout delle traduzioni correnti, ma questa opzione non è consigliata in quanto la creazione di nuove connessioni con le nuove regole può causare un comportamento imprevisto.

Nota: se si desidera bloccare il traffico dall'area di sicurezza superiore (interna) all'area di sicurezza inferiore (Internet/DMZ), creare un ACL e applicarlo all'interfaccia interna dell'appliance PIX/ASA come in entrata.

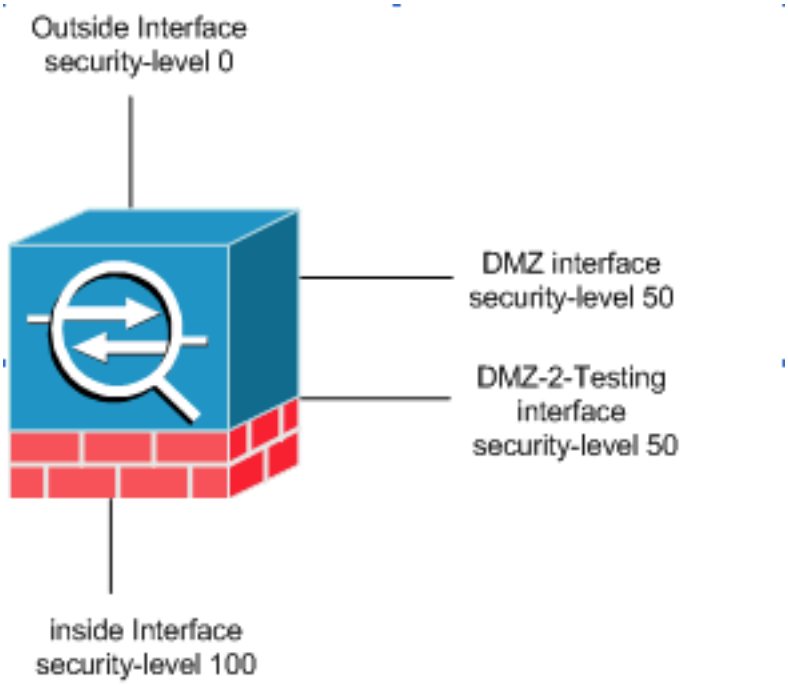
Nota: Esempio: Per bloccare la porta 80 dal traffico 172.20.1.100 dell'host sulla rete interna verso

Internet, utilizzare questo comando:

```
ASA-AIP-CLI(config)#access-list InsidetoOutside extended deny tcp host 172.20.1.100 any eq www
ASA-AIP-CLI(config)#access-list InsidetoOutside extended permit tcp any any
ASA-AIP-CLI(config)#access-group InsidetoOutside in interface inside
```

Comunicazione con lo stesso livello di sicurezza

La configurazione iniziale mostra che le interfacce "DMZ" e "DMZ-2-testing" sono configurate con il livello di sicurezza (50); per impostazione predefinita, queste due interfacce non possono comunicare. Di seguito vengono indicate le interfacce che possono comunicare con questo comando:




```
ASA-AIP-CLI(config)# same-security-traffic permette di interfacciarsi
```

Nota: anche se l'interfaccia "same-security traffic allow inter-interface" è stata configurata per le stesse interfacce di livello di sicurezza ("DMZ" e "DMZ-2-testing"), è comunque necessaria una regola di conversione (statica/dinamica) per accedere alle risorse posizionate in tali interfacce.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Risoluzione dei problemi di connessione tramite PIX e ASA
- Configurazioni NATerifica NAT e risoluzione dei problemi

Informazioni correlate

- Guida di riferimento ai comandi di Cisco ASA
- Guida di riferimento ai comandi di Cisco PIX

- Messaggi di errore e di sistema Cisco ASA
- Messaggi di errore e di sistema Cisco PIX
- Documentazione e supporto tecnico – Cisco Systems