Sécurisation des réseaux avec des VLAN privés et des listes de contrôle d'accès VLAN

Contenu

Introduction

L’un des principaux facteurs de conception réussie en matière de sécurité du réseau consiste à identifier et exécuter un modèle de confiance approprié. Le modèle de confiance approprié définit qui doit communiquer avec qui, ainsi que le type de besoins en termes d’échange de trafic ; tout autre trafic doit être refusé. Une fois que le modèle de confiance approprié a été identifié, le concepteur du système de sécurité doit décider comment l’exécuter. Comme davantage de ressources stratégiques sont globalement disponibles et que les nouvelles formes d’attaque réseau évoluent, l’infrastructure de sécurité réseau tend à devenir plus sophistiquée et davantage de produits sont disponibles. Les pare-feux, les routeurs, les commutateurs LAN, les systèmes de détection d’intrusion, les serveurs AAA et les VPN constituent une partie des technologies et des produits qui permettent d’exécuter le modèle. Naturellement, chacun de ces produits et technologies joue un rôle particulier dans la mise en œuvre d’un système de sécurité global et il est essentiel que le concepteur comprenne comment ces éléments peuvent être déployés.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Ce document décrit les configurations PVLAN sur des commutateurs fonctionnant sous CatOS uniquement. Pour consulter des exemples de configuration parallèle des PVLAN sur les commutateurs fonctionnant sous Cisco IOS et CatOS, consultez le document Configuration de VLAN privés isolés sur les commutateurs Catalyst.

Les PVLAN ne sont pas pris en charge par tous les commutateurs et toutes les versions logicielles. Consultez le Tableau de prise en charge des commutateurs Catalyst de VLAN privé pour déterminer si votre plate-forme et votre version logicielles prennent en charge les PVLAN.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Informations générales

L'identification et l'exécution d'un modèle de confiance approprié semblent être une tâche particulièrement élémentaire. Pourtant, après plusieurs années de mise en œuvre de systèmes de sécurité, nous savons par expérience que les incidents liés à la sécurité découlent fréquemment de conceptions de système de sécurité de mauvaise qualité. En règle générale, ces conceptions de mauvaise qualité relèvent de la non-exécution d'un modèle de confiance approprié qui peut découler d'une incompréhension des éléments nécessaires ou encore d'une incompréhension et d'une utilisation erronée des technologies impliquées.

Ce document explique en détail comment deux fonctionnalités disponibles dans nos commutateurs Catalyst, VLAN privés (PVLAN) et Listes de contrôle d'accès au VLAN (VACL), permettent de vérifier qu'un modèle de confiance est adapté à l'entreprise et aux environnements du prestataire de services.

Importance d'exécuter un modèle de confiance approprié

Conséquence immédiate de la non-exécution d'un modèle de confiance adéquat, la mise en œuvre d'un système de sécurité global est moins protégée contre les activités malveillantes. Des zones démilitarisées (DMZs) sont généralement mises en œuvre sans mise en place de politiques appropriées, ce qui facilite l'activité d'un intrus potentiel. Cette section analyse comment les DMZs sont généralement mises en place et les conséquences d'une conception de faible qualité. Nous expliquerons plus tard comment atténuer, ou dans le meilleur cas éviter, ces conséquences.

En règle générale, les serveurs DMZ ne sont supposés traiter que les requêtes en provenance d'Internet, voire lancer la connexion à quelques serveurs principaux situés dans un autre segment DMZ, tel qu'un serveur de base de données. Dans le même temps, les serveurs DMZ ne sont pas supposés communiquer entre eux ni lancer une connexion externe. Ceci définit clairement les flux de trafic nécessaires dans un modèle de confiance simple ; cependant, nous constatons fréquemment que ce genre de modèle n'est pas correctement exécuté.

Les concepteurs tendent généralement à mettre en œuvre les DMZs à l'aide d'un segment commun à tous les serveurs sans aucun contrôle de trafic entre elles. Par exemple, tous les serveurs sont situés dans un VLAN commun. Comme le trafic n'est pas contrôlé au sein du même VLAN, si l'un des serveurs est compromis, il peut servir de base pour attaquer n'importe quels autres serveurs et hôtes appartenant au même segment. Ceci facilite considérablement l'activité

d’un intrus potentiel qui peut ainsi effectuer une redirection de port ou attaquer une couche applicative.

En règle générale, les pare-feux et les filtres de paquet ne sont utilisés que pour contrôler les connexions entrantes, mais aucune action n’est mise en place pour restreindre les connexions provenant de la DMZ. Il y a quelques temps, une vulnérabilité bien connue dans un script de cgi-bin a permis à un intrus d’ouvrir une session X-term en envoyant simplement un flux HTTP ; ce type de trafic doit être autorisé par le pare-feu. Si l’intrus a suffisamment de chance, il peut utiliser une autre menace pour obtenir une invite racine, en règle générale, une attaque de type dépassement de mémoire tampon. La plupart du temps, ces genres de problèmes peuvent être évités en exécutant un modèle de confiance approprié. Tout d’abord, les serveurs ne sont pas supposés communiquer entre eux, ensuite, aucune connexion ne peut être initiée depuis ces serveurs vers l’extérieur.

Les mêmes commentaires s’appliquent à beaucoup d’autres scénarios, depuis n’importe quel segment non sécurisé classique jusqu’aux batteries de serveurs des prestataires de services d’applications.

Les PVLANs et les VACLs sur les commutateurs Catalyst peuvent faciliter la mise en place d’un modèle de confiance approprié. Les PVLAN permettent de restreindre le trafic entre les hôtes d’un même segment tandis que les VACL le facilitent en offrant un meilleur contrôle du flux de trafic provenant d’un ou destiné à un segment particulier. Ces fonctionnalités sont traitées dans les sections suivantes.

VLAN privés

Les PVLAN sont disponibles sur le commutateur Catalyst 6000 fonctionnant sous CatOS 5.4 ou version ultérieure et sur les commutateurs Catalyst 4000, 2980G, 2980G-A, 2948G et 4912G fonctionnant sous CatOS 6.2 ou version ultérieure.

De notre point de vue, les PVLAN sont un outil qui permet d’isoler le trafic de la couche L2 en transformant un segment de diffusion en un segment de type multi-accès sans diffusion. Le trafic transmis à un commutateur depuis un port proche (c’est-à-dire, un port qui est capable de transférer le trafic des VLAN principaux et secondaires) peut être transféré vers tous les ports appartenant au même VLAN principal. Le trafic transmis à un commutateur depuis un port dirigé vers un VLAN secondaire (VLAN isolé, VLAN communautaire, ou VLAN communautaire bidirectionnel) peut être transféré à un port proche ou à un port appartenant au même VLAN communautaire. Les échanges de trafic entre plusieurs ports dirigés vers le même VLAN isolé sont impossibles.

L’image suivante présente le concept.

Figure 1 : VLAN privés

Le VLAN principal est représenté en bleu ; les VLAN secondaires sont représentés en rouge et jaune. L’hôte 1 est connecté à un port du commutateur qui appartient au VLAN secondaire rouge. L’hôte 2 est connecté à un port du commutateur qui appartient au VLAN secondaire jaune.

Lors de la transmission d’un hôte, le trafic transite par le VLAN secondaire. Par exemple, le trafic de l’hôte 2 en mode de transmission passe par le VLAN jaune. Quand ces serveurs sont en mode de réception, le trafic transite par le VLAN bleu, c’est-à-dire le VLAN principal.

Les ports auxquels les routeurs et les pare-feux sont connectés sont des ports proches car ils peuvent transférer le trafic en provenance de chaque VLAN secondaire défini dans l'application, ainsi que du VLAN principal. Les ports connectés à chaque hôte ne peuvent transférer que le trafic en provenance du VLAN principal et du VLAN secondaire configurés sur ce port.

L'illustration représente les VLAN privés sous la forme de câbles reliant les routeurs et les hôtes : Le câble qui entoure tous les autres correspond au VLAN principal (bleu). Le trafic sur le VLAN bleu circule des routeurs vers les hôtes. Les câbles internes au VLAN primaire correspondent aux VLAN secondaires. Le trafic circule des hôtes vers le routeur.

Comme l'indique l'illustration, un VLAN principal peut contenir un ou plusieurs VLAN secondaires.

Précédemment dans ce document, nous avons dit que les PVLANs facilitent l'exécution d'un modèle de confiance approprié en garantissant simplement l'isolement des hôtes dans un segment commun. Maintenant que nous en savons plus sur les VLAN privés, voyons comment les implémenter dans notre scénario DMZ initial. Les serveurs ne sont pas supposés communiquer entre eux ; par contre, ils doivent communiquer avec le pare-feu ou le routeur auquel ils sont connectés. Dans ce cas, les serveurs doivent être connectés aux ports isolés tandis que les routeurs et les pare-feux sont reliés aux ports proches. Le cas échéant, si l'un des serveurs est compromis, l'intrus ne peut pas utiliser le même serveur pour attaquer un autre serveur au sein du même segment. Le commutateur émet n'importe quel paquet à la vitesse du câble, sans baisse de performances.

Autre élément important, ce type de contrôle ne peut être implémenté qu'au niveau d'un périphérique L2 car tous les serveurs appartiennent au même sous-réseau. Le pare-feu ou le routeur sont inutiles car les serveurs essaient de communiquer directement. Une autre option consiste à dédier un port de pare-feu par serveur, mais cette solution est probablement trop onéreuse, difficile à mettre en œuvre et non évolutive.

Dans une section ultérieure, nous décrivons en détail d'autres scénarios types dans lesquels vous pouvez utiliser cette fonctionnalité.

Listes de contrôle d'accès au VLAN

Les VACL sont disponibles sur le commutateur Catalyst 6000 fonctionnant sous CatOS 5.3 ou version ultérieure.

Les VACLs peuvent être configurées sur un commutateur Catalyst 6500 au niveau de la couche L2 sans qu'un routeur ne soit nécessaire (vous avez seulement besoin d'une carte de fonctionnalités de politique (PFC)). Elles fonctionnent à la vitesse du câble. Par conséquent, la configuration des VACL sur un commutateur Catalyst 6500 n'entraîne aucune baisse des performances. La recherche des VACL étant exécutée au niveau matériel indépendamment de la taille de la liste d'accès, le débit de transfert reste inchangé.

Les VACL peuvent être dirigées séparément vers les VLAN principaux ou secondaires. La configuration d'un VACL sur un VLAN secondaire permet de filtrer le trafic provenant des hôtes sans toucher au trafic généré par les routeurs ou les pare-feux.

En combinant les VACL et les VLAN privés, il est possible de filtrer le trafic en fonction du sens du trafic. Par exemple, si deux routeurs sont connectés au même segment en tant qu'hôtes (serveurs, par exemple), vous pouvez configurer les VACL sur des VLAN secondaires de sorte que seul le trafic généré par les hôtes est filtré tandis que le trafic entre les routeurs reste intact.

Vous pouvez facilement déployer les VACLs pour exécuter le modèle de confiance approprié. Analysons notre DMZ. Les serveurs au niveau du DMZ sont supposés ne prendre en charge que les connexions entrantes. Ils ne sont pas supposés initier de connexions sortantes. Une VACL peut être appliquée à leur VLAN secondaire afin de contrôler le trafic émis par ces serveurs. Notez que si vous utilisez des VACL, le trafic est abandonné au niveau matériel de sorte qu'il n'affecte pas le CPU du routeur ou du commutateur. Même si l'un des serveurs est affecté par un déni de service distribué (DDoS) en tant que source, le commutateur supprime tout trafic illégitime à la vitesse du câble sans baisse des performances. Des filtres semblables peuvent être appliqués au niveau du routeur ou du pare-feu auquel les serveurs sont connectés mais en règle générale, cela affecte considérablement les performances.

Les ACL basées sur Mac ne fonctionnent pas correctement avec le trafic IP. Par conséquent, il n'est pas recommandé de surveiller les PVLAN depuis des VACL.

Limitations connues des VACLs et des PVLANs

Lors de la configuration du filtrage avec les VACL, vous devez manipuler le fragment avec précaution sur le PFC et vous assurer que la configuration est conforme aux spécifications matérielles.

Au vue de la conception matérielle du PFC du superviseur 1 du commutateur Catalyst 6500, il est préférable de refuser explicitement les fragments d'ICMP. De fait, les fragments d'ICMP (Internet Control Message Protocol) et la réponse d'écho sont considérés comme identiques par le matériel, ce dernier étant par défaut programmé pour autoriser explicitement les fragments. Par conséquent, pour interrompre la transmission des paquets de réponses d'écho à partir des serveurs, vous devez configurer cette interdiction explicitement avec la ligne **deny icmp any any fragment**. Les configurations dans ce document prennent en compte cet élément.

Il existe une limitation de sécurité bien connue au niveau des PVLAN : la possibilité qu'un routeur retourne le trafic au sous-réseau duquel il provient. Un routeur peut acheminer le trafic via des ports isolés allant à l'encontre de l'objectif des PVLAN. Cette limitation résulte du fait que les PVLAN sont un outil qui isole la couche L2, mais pas la couche L3.

La retransmission par le chemin inverse de monodiffusion (Unicast Reverse Path Forwarding, uRPF) ne fonctionne pas bien avec les ports hôte PVLAN, ainsi l'uRPF ne doit pas être utilisée en combination avec un PVLAN.

Pour résoudre ce problème, il suffit de configurer les VACL sur les VLAN principaux. L'étude de cas fournit les VACL à configurer sur le VLAN principal pour abandonner le trafic provenant du même sous-réseau et réacheminé au même sous-réseau.

Sur certaines cartes de ligne, la configuration des applications PVLAN/ports d'agrégation dépend de certaines restrictions lorsqu'il est nécessaire pour les configurer que plusieurs applications PVLAN appartiennent à différents circuits intégrés à application spécifique. Ces restrictions sont supprimées sur le nouveau port ASIC Coil3. Consultez la section sur la configuration logicielle de la documentation du dernier commutateur Catalyst pour en savoir plus.

Exemples d'études de cas

La section suivante décrit trois études de cas qui nous semblent représentatives de la plupart des mises en œuvre et qui fournissent des détails relatifs au déploiement de la sécurité des PVLAN et

des VACL.

Ces scénarios sont les suivants :

- DMZ d'intercommunication
- DMZ externe
- Concentrateur VPN en parallèle du pare-feu

DMZ d'intercommunication

Il s'agit de l'un des scénarios les plus fréquemment déployés. Dans cet exemple, la DMZ est mise en œuvre comme une zone de transit entre deux routeurs pare-feux comme illustré ci-après.

Figure 2 : DMZ d'intercommunication

Dans cet exemple, les utilisateurs externes et internes peuvent accéder aux serveurs DMZ ; par contre, les serveurs n'ont pas besoin de communiquer entre eux. Dans certains cas, les serveurs DMZ doivent ouvrir une connexion vers un hôte interne. Dans le même temps, les clients internes doivent pouvoir accéder à Internet sans restrictions. Dans un bon exemple, les serveurs Web au niveau de la DMZ doivent pouvoir communiquer avec un serveur de base de données intégré au réseau tout en autorisant les clients internes à accéder à Internet.

Le pare-feu externe est configuré pour autoriser les connexions entrantes vers les serveurs au niveau de la DMZ. Cependant, en règle générale, aucun filtre ni aucune restriction ne sont appliqués au trafic sortant, notamment au trafic provenant de la DMZ. Comme indiqué précédemment dans ce document, ceci peut éventuellement simplifier l'activité d'un intrus pour deux raisons : tout d'abord, dès que l'un des hôtes DMZ est compromis, tous les autres hôtes DMZ sont exposés ; ensuite, un intrus peut facilement exploiter une connexion sortante.

Comme les serveurs DMZ n'ont pas besoin de communiquer entre eux, nous vous recommandons de vérifier qu'ils sont isolés au niveau de la couche L2. Pour ce faire, définissez les ports des serveurs comme étant des ports PVLAN isolés tous en définissant les ports se connectant aux deux pare-feux comme étant des ports proches. De cette manière, vous définirez un VLAN principal pour les pare-feux et un VLAN secondaire pour les serveurs DMZ.

Les VACL sont utilisées pour contrôler le trafic provenant de la DMZ. De cette manière, aucun intrus ne peut ouvrir de connexion sortante illégitime. N'oubliez pas que les serveurs DMZ doivent non seulement répondre au trafic correspondant aux sessions des clients, mais également assurer des services supplémentaires, comme le système DNS (système de noms de domaine) et la découverte de l'unité de transmission maximale (MTU) du chemin d'accès. Ainsi, l'ACL doit autoriser tous les services requis par les serveurs DMZ.

Test de la DMZ d'intercommunication

Nous avons implémenté dans nos bancs d'essai un segment DMZ intégrant deux routeurs configurés en tant que serveurs de test, server_dmz1 et server_dmz2. Ces serveurs doivent être accessibles par les clients externes et internes et toutes les connexions HTTP sont authentifiées à l'aide d'un serveur RADIUS interne (CiscoSecure ACS pour UNIX). Les routeurs internes et externes sont configurés en tant que pare-feux assurant un filtrage par paquet. L'illustration suivante présente le banc d'essai, y compris le système d'adressage utilisé.

Figure 3 : Banc d'essai de la DMZ d'intercommunication

La liste suivante regroupe les étapes essentielles de configuration des PVLAN. Le Catalyst 6500 est utilisé en tant que commutateur L2 dans la DMZ.

- Server_dmz_1 est connecté au port 3/9
- Server_dmz_2 est connecté au port 3/10
- Le routeur interne est connecté au port 3/34
- Le routeur externe est connecté au port 3/35

Nous avons choisi les VLANs suivants :

- 41 correspond au VLAN principal
- 42 correspond au VLAN isolé

Configuration d'un VLAN privé

La configuration suivante définit les PVLAN sur les ports impliqués.

```
ecomm-6500-2 (enable) set vlan 41 pvlan primary
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 41 configuration successful

ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      -         -
ecomm-6500-2 (enable) set vlan 42 pvlan isolated
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 42 configuration successful
ecomm-6500-2 (enable) set pvlan 41 42 3/9-10
Successfully set the following ports to Private Vlan 41,42:
3/9-10

ecomm-6500-2 (enable) set pvlan mapping 41 42 3/35
Successfully set mapping between 41 and 42 on 3/35
ecomm-6500-2 (enable) set pvlan mapping 41 42 3/34
Successfully set mapping between 41 and 42 on 3/34

Port  Name                 Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/9  server_dmz1       connected  41,42      a-half  a-10 10/100BaseTX
 3/10 server_dmz2       connected  41,42      a-half  a-10 10/100BaseTX

 3/34 to_6500_1         connected   41        auto  auto 10/100BaseTX
 3/35 external_router_dm connected  41        a-half  a-10 10/100BaseTX
```

Configuration d'une VACL sur le VLAN principal

Cette section est indispensable pour améliorer la sécurité sur la DMZ. Comme indiqué dans la section Limitations connues des VACL et des PVLAN, même si les serveurs appartiennent à deux VLAN secondaires différents ou au même VLAN isolé, un intrus peut toujours trouver un moyen de les faire communiquer entre eux. Si les serveurs essayent de communiquer directement, la communication sera bloquée au niveau de la couche L2 grâce aux PVLANs. Si les serveurs sont compromis, puis configurés par un intrus de sorte que le trafic d'un même sous-réseau est transmis au routeur, ce dernier réachemine le trafic sur le même sous-réseau, allant ainsi à l'encontre de l'objectif des PVLAN.

Par conséquent, vous devez configurer une VACL sur le VLAN principal (le VLAN qui transmet le trafic des routeurs) en appliquant les stratégies suivantes :

- Autoriser le trafic dont l'IP source correspond à l'IP du routeur
- Refuser le trafic dont les IP source et de destination appartiennent au sous-réseau DMZ
- Autoriser le trafic restant

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
------------------------------------------------
1. permit ip host 172.16.65.193 any
2. permit ip host 172.16.65.201 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any

ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
```

Cette ACL n'affectera pas le trafic généré par les serveurs ; il empêchera uniquement les routeurs de réacheminer le trafic en provenance des serveurs vers le même VLAN. Les deux premiers énoncés permettent aux routeurs d'envoyer des messages de type redirection d'ICPM ou inaccessibilité d'ICMP aux serveurs.

Configuration d'une VACL sur le VLAN secondaire

Les journaux de configuration suivants permettent de montrer comment nous configurons un VACL pour filtrer le trafic généré par les serveurs. En configurant cette VACL, nous voulons obtenir le résultat suivant :

- Autoriser le **ping** à partir des serveurs (autoriser l'**écho**)
- Bloquer l'envoi de réponses d'**écho** à partir des serveurs
- Autoriser les connexions HTTP provenant de l'extérieur
- Autoriser l'authentification RADIUS (port UDP 1645) et le trafic de gestion des comptes (port UDP 1646)
- Autoriser le trafic DNS (port UDP 53)

Nous voulons bloquer le reste du trafic.

Concernant la fragmentation sur le segment du serveur, nous supposons que :

- Les serveurs ne génèreront pas de trafic fragmenté
- Les serveurs sont susceptibles de recevoir du trafic fragmenté

Compte tenu de la conception matérielle du PFC du Supervisor 1 du commutateur Catalyst 6500, il est préférable de refuser explicitement les fragments d'ICMP. En effet les fragments d'ICMP et la réponse d'écho sont considérés comme identiques par le matériel, ce dernier étant par défaut programmé pour autoriser explicitement les fragments. Par conséquent, pour interrompre la transmission des paquets de réponse d'écho à partir des serveurs, vous devez configurer cette interdiction explicitement avec la ligne **deny icmp any any fragment**.

```
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out deny icmp any any fragment
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.199 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.202 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.199 eq 80 any
established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.202 eq 80 any
established
```

```
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199 any eq 53
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202 any eq 53

ecomm-6500-2 (enable) Commit sec acl all

ecomm-6500-2 (enable) Set sec acl map dmz_servers_out 42

ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
dmz_servers_out                  IP   42

ecomm-6500-2 (enable) sh sec acl info dmz_servers_out
set security acl ip dmz_servers_out
------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 172.16.65.199 any echo
3. permit icmp host 172.16.65.202 any echo
4. permit tcp host 172.16.65.199 eq 80 any established
5. permit tcp host 172.16.65.202 eq 80 any established
6. permit udp host 172.16.65.199 eq 1645 host 172.16.171.9 eq 1645
7. permit udp host 172.16.65.202 eq 1645 host 172.16.171.9 eq 1645
8. permit udp host 172.16.65.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 172.16.65.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 172.16.65.199 any eq 53
11. permit udp host 172.16.65.202 any eq 53
```

Test de la configuration

La sortie suivante a été capturée alors que les PVLAN étaient configurés mais qu'aucune VACL n'était encore appliquée. Ce test montre que l'utilisateur peut lancer un **ping** sur le routeur interne et les serveurs depuis le routeur externe.

```
external_router#ping 172.16.65.193
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!

external_router#ping 172.16.65.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
external_router#ping 172.16.65.199
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

L'exemple suivant montre que nous pouvons lancer un **ping** à partir des serveurs sur le réseau externe et la passerelle par défaut mais pas sur les serveurs appartenant au même VLAN secondaire.

```
server_dmz1#ping 203.5.6.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.5.6.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

server_dmz1#ping 172.16.65.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Après l'application des VACL, l'exécution d'un ping à partir du routeur externe échoue :

```
external_router#ping 172.16.65.199
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

L'exemple suivant montre le serveur recevant des requêtes HTTP GET du réseau interne :

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
```

```
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

DMZ externe

Le scénario relatif à la DMZ externe est probablement la mise en œuvre la mieux acceptée et la plus largement déployée. Une DMZ externe est mise en œuvre à l'aide d'une ou plusieurs interfaces d'un pare-feu, comme illustré ci-après.

Figure 4 : DMZ externe

En règle générale, les spécifications requises par les DMZ tendent à être identiques indépendamment de la mise en œuvre conceptuelle. Comme indiqué dans le cas précédent, les serveurs DMZ doivent normalement être accessibles tant par les clients externes que par le réseau interne. Les serveurs DMZ nécessiteront probablement d'accéder à certaines ressources internes. Par ailleurs, ils ne sont pas supposés communiquer entre eux. Dans le même temps, aucun trafic ne doit être initié de la DMZ vers Internet ; ces serveurs DMZ ne doivent répondre qu'au trafic correspondant aux connexions entrantes.

Comme dans l'étude de cas précédente, la première étape de configuration consiste à isoler la couche L2 à l'aide de PVLAN tout en veillant à ce que les serveurs DMZ ne puissent pas communiquer entre eux sans bloquer l'accès des hôtes internes et externes aux serveurs. Pour ce faire, il est nécessaire de configurer les serveurs dans un VLAN secondaire à l'aide de ports isolés. Vous devez définir le pare-feu dans un VLAN principal avec un port proche. Le pare-feu est le seul périphérique dans ce VLAN principal.

La seconde étape consiste à définir les ACL pour contrôler le trafic provenant de la DMZ. Lors de la définition de ces ACL, nous devons nous assurer que seul le trafic requis est autorisé.

Test de la DMZ externe

L'illustration ci-après montre le banc d'essai mis en œuvre dans le cadre de cette étude de cas dans laquelle nous avons utilisé un pare-feu PIX avec une troisième interface pour la DMZ. Le même groupe de routeurs est utilisé en tant que serveurs Web et toutes les sessions HTTP sont authentifiées avec le même serveur RADIUS.

Figure 5 : Banc d'essai de la DMZ externe

Dans ce scénario, seuls les éléments les plus intéressants sont développés à l'exception des fichiers de configuration, les PVLAN et les configurations des VACL ayant été présentés dans l'étude de cas précédente.

Configuration PIX

```
server_dmz1#debug ip http url
```

```
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

Configuration RADIUS

Configuration NAS

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
```

```
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

Serveur RADIUS CSUX

```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
```

```
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

Configuration d'un Catalyst

Notez que dans cette configuration, il n'est pas nécessaire de configurer une VACL sur le VLAN principal car le PIX ne redirige pas le trafic hors de l'interface de laquelle il provient. Une VACL telle que celle qui est décrite dans la section Configuration d'une VACL sur le VLAN principal doit être redondante.

```
set security acl ip dmz_servers_out
---------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established
6. permit udp host 199.5.6.199 eq 1645 host 172.16.171.9 eq 1645
7. permit udp host 199.5.6.202 eq 1645 host 172.16.171.9 eq 1645
8. permit udp host 199.5.6.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 199.5.6.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 199.5.6.199 any eq 53
11. permit udp host 199.5.6.202 any eq 53
ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      42        isolated         3/9-10

ecomm-6500-2 (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
 3/14 41      42
 3/34 41      42
 3/35 41      42
ecomm-6500-2 (enable) sh port
Port  Name               Status     Vlan       Duplex Speed Type
```

```
----- ----------------- ---------- ---------- ------ ----- ------------
 3/9  server_dmz1        connected  41,42      a-half  a-10 10/100BaseTX
 3/10 server_dmz2        connected  41,42      a-half  a-10 10/100BaseTX
 3/14 to_pix_port_2      connected  41           full   100 10/100BaseTX
 3/35 external_router_dm notconnect 41           auto  auto 10/100BaseTX
```

Concentrateur VPN en parallèle du pare-feu

Lors de la mise en œuvre de réseaux privés virtuels (VPN) Access, la conception parallèle est sans conteste l'une des approches favorites (voir l'illustration ci-après). Les clients préfèrent généralement cette approche de conception car sa mise en œuvre est aisée et n'a que très peu d'incidence sur l'infrastructure existante. Par ailleurs, elle très facilement évolutive car elle repose sur la flexibilité des périphériques.

Dans l'approche parallèle, le concentrateur VPN se connecte aux segments internes et externes. Toutes les sessions VPN se terminent au niveau du concentrateur sans passer par le pare-feu. En règle générale, les clients VPN disposent d'un accès illimité au réseau interne, mais il arrive que leur accès soit restreint à un ensemble de serveurs internes (batterie de serveurs). L'une des caractéristiques souhaitables consiste à isoler le trafic VPN du trafic Internet standard pour, par exemple, ne pas autoriser les clients VPN à accéder à Internet par l'intermédiaire du pare-feu de l'entreprise.

Figure 6 : Concentrateur VPN en parallèle du pare-feu

Test du concentrateur VPN en parallèle du pare-feu

Dans cet exemple, nous avons utilisé un concentrateur VPN 5000 installé parallèlement à un pare-feu PIX. Les deux routeurs configurés en tant que serveurs Web ont été installés au niveau du segment interne en tant que batterie de serveurs internes. Les clients VPN ne sont autorisés à accéder qu'aux batteries de serveurs et le trafic Internet doit être isolé du trafic VPN (IPSec). La figure F26297ci-après présente le banc d'essai.

Figure 7 : Concentrateur VPN en parallèle du banc d'essai de pare-feu

Dans ce scénario, nous nous intéressons à deux éléments importants :

- Le commutateur L2 interne
- Le commutateur L2 externe

Les flux de trafic du commutateur L2 interne sont définis en fonction des énoncés suivants :

- Les clients VPN disposent d'un accès complet à un ensemble prédéfini de serveurs internes (batterie de serveurs)
- Les clients internes sont également autorisés à accéder à la batterie de serveurs
- Les clients internes bénéficient d'un accès illimité à Internet
- Le trafic provenant du concentrateur VPN doit être isolé du pare-feu PIX

Les flux de trafic du commutateur L2 externe sont définis comme suit :

- Il doit être possible de transmettre le trafic provenant du routeur au concentrateur VPN ou au PIX
- Le trafic provenant du PIX doit être isolé du trafic provenant du VPN

Par ailleurs, il est possible que l'administrateur souhaite empêcher la transmission du trafic au sein du réseau interne vers les hôtes VPN. Pour ce faire, il suffit de configurer les VACL sur le

VLAN principal (la VACL filtrera uniquement le trafic provenant du routeur interne ; le reste du trafic ne sera pas affecté).

Configuration PVLAN

Comme le principal objectif de cette conception est de maintenir le trafic issu du PIX isolé du trafic provenant des serveurs et du concentrateur VPN, nous configurons le PIX sur un PVLAN différent de celui sur lequel les serveurs et le concentrateur VPN sont configurés.

Le trafic provenant du réseau interne doit pouvoir accéder à la batterie de serveurs, ainsi qu'au concentrateur VPN et au PIX. Par conséquent, le port qui se connecte au réseau interne est un port proche.

Les serveurs et le concentrateur VPN appartiennent au même VLAN secondaire car ils pourront communiquer entre eux.

De même que le commutateur L2 externe, le routeur qui permet d'accéder à Internet (et qui appartient généralement à un prestataire de services Internet (ISP)) est connecté à un port proche tandis que le concentrateur VPN et le PIX appartiennent aux mêmes VLANs privés et isolés (de sorte que tout échange de trafic est impossible). De cette manière, le trafic qui provient du prestataire de services peut emprunter l'accès au concentrateur VPN ou au PIX. Le PIX et le concentrateur VPN bénéficient d'une meilleure protection car ils sont isolés.

Configuration PVLAN du commutateur L2 interne

```
sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- -----------
41      42        community        3/7,3/9-10
41      43        isolated         3/12

ecomm-6500-2 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/34 41      42-43

ecomm-6500-2 (enable) sh port 3/7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/7  to_vpn_conc        connected  41,42      a-half  a-10 10/100BaseTX

ecomm-6500-2 (enable) sh port 3/9
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/9  server_1           connected  41,42      a-half  a-10 10/100BaseTX


ecomm-6500-2 (enable) sh port 3/10
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/10 server_2           connected  41,42      a-half  a-10 10/100BaseTX

ecomm-6500-2 (enable) sh port 3/12
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/12 to_pix_intf1       connected  41,43      a-full a-100 10/100BaseTX
```

```
ecomm-6500-2 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/34 41      42-43

ecomm-6500-2 (enable) sh port 3/34
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/34 to_int_router      connected  41         a-full a-100 10/100BaseTX
```

Configuration PVLAN du commutateur L2 externe

```
sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      45        isolated         3/7,3/33

ecomm-6500-1 (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
 3/43 41      45

ecomm-6500-1 (enable) sh port 3/7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/7  from_vpn           connected  41,45      a-half  a-10 10/100BaseTX

ecomm-6500-1 (enable) sh port 3/33
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/33 to_pix_intf0       connected  41,45      a-full a-100 10/100BaseTX

ecomm-6500-1 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/43 41      45
ecomm-6500-1 (enable) sh port 3/43
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/43 to_external_router connected  41         a-half  a-10 10/100BaseTX
```

Test de la configuration

Cette expérience montre que le routeur interne peut transiter par le pare-feu et atteindre le routeur externe (routeur de pare-feu externe dont l'interface est 198.5.6.1).

```
ping 198.5.6.1
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Cette expérience montre les capacités du serveur 1 :

- Le serveur 1 peut envoyer un ping au routeur interne :`server_1#`**`ping 172.16.65.193`**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- Le serveur 1 peut envoyer un ping au VPN :`server_1#`**`ping 172.16.65.203`**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.203, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- Le serveur 1 ne peut pas envoyer un ping à l'interface PIX interne :`server_1#`**`ping 172.16.65.201`**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.201, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

- Le serveur 1 ne peut pas envoyer un ping au routeur externe :`server_1#`**`ping 198.5.6.1`**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

L'expérience suivante montre qu'il est possible d'ouvrir des sessions HTTP à partir du réseau interne vers la batterie de serveurs.

```
server_1#ping 198.5.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

L'expérience suivante montre que le trafic HTTP du réseau VPN peut atteindre la batterie de serveurs (adresse 10.1.1.1).

```
server_1#ping 198.5.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Voici la configuration du concentrateur VPN :

```
server_1#ping 198.5.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

La commande suivante indique la liste des utilisateurs connectés :

```
sh VPN user
Port        User            Group           Client          Local           ConnectNumber
                                            Address         Address         Time
-------------------------------------------------------------------------------
VPN 0:1     martin          RemoteUsers     206.1.1.10      10.1.1.1        00:00:11:40
```

Notez que la passerelle par défaut sur les serveurs correspond au routeur interne 172.16.65.193 qui émettra une redirection d'ICMP vers 172.16.65.203. Cette mise en œuvre nuit à l'optimisation du flux de trafic car l'hôte peut envoyer le premier paquet d'un flux au routeur et, à la réception de la redirection, transmettre les autres paquets à la passerelle, mieux adaptée pour prendre en charge ce trafic. De plus, il est possible de configurer deux routes différentes sur les serveurs eux-

mêmes afin de pointer le VPN sur les adresses 10.x.x.x et l'adresse 172.16.65.193 pour le reste du trafic. Si seule la passerelle par défaut est configurée sur les serveurs, nous devons vérifier que l'interface du routeur est configurée avec « ip redirect ».

Nous avons constaté le point intéressant suivant pendant le test. Si nous essayons d'envoyer un **ping** à une adresse externe telle que 198.5.6.1 à partir des serveurs ou du VPN, la passerelle par défaut l'envoie, puis l'ICPM le redirige vers 172.16.65.201.

```
sh VPN user
Port        User            Group           Client          Local           ConnectNumber
                                            Address         Address         Time
-------------------------------------------------------------------------------
VPN 0:1     martin          RemoteUsers     206.1.1.10      10.1.1.1        00:00:11:40
```

Àce stade, les serveurs ou le VPN envoient une requête ARP (Protocole de résolution d'adresse) à 172.16.65.201 et ne reçoivent pas de réponse en retour de 201, cette dernière figurant sur un autre VLAN secondaire ; c'est ce que le PVLAN nous fournit. En réalité, il est facile de contourner ce problème. Il suffit d'envoyer le trafic au MAC de .193 avec l'IP de destination 172.16.65.201.

Le routeur .193 réachemine le trafic à la même interface. Cependant, comme l'interface du routeur est un port proche, le trafic parvient à .201, ce que nous voulons éviter. Ce problème a été expliqué dans la section Limitations connues des VACLs et des PVLANs .

Configuration VACL

Cette section est cruciale pour améliorer la sécurité de la batterie de serveurs. Comme indiqué dans la section Limitations connues des VACL et des PVLAN, même si les serveurs et le PIX appartiennent à deux VLAN secondaires différents, il existe encore une méthode qu'un intrus peut utiliser pour les faire communiquer entre eux. S'ils essayent de communiquer directement, les PVLANs les en empêcheront. Si les serveurs sont compromis, puis configurés par un intrus de sorte que le trafic d'un même sous-réseau est transmis au routeur, ce dernier réachemine le trafic sur le même sous-réseau, allant ainsi à l'encontre de l'objectif des PVLAN.

Par conséquent, vous devez configurer une VACL sur le VLAN principal (le VLAN qui transmet le trafic des routeurs) en appliquant les stratégies suivantes :

- Autoriser le trafic dont l'IP source correspond à l'IP du routeur
- Refuser le trafic avec les IP source et de destination appartenant au sous-réseau de la batterie de serveurs
- Autoriser le trafic restant

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
------------------------------------------------
1. permit ip host 172.16.65.193 any
2. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
3. permit ip any any

ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
```

Cette ACL n'affectera pas le trafic généré par les serveurs ou le PIX ; il empêchera uniquement les routeurs de réacheminer le trafic en provenance des serveurs vers le même VLAN. Les deux premiers énoncés permettent aux routeurs d'envoyer des messages de type redirection d'ICPM

ou inaccessibilité d'ICMP aux serveurs.

Nous avons identifié un autre flux de trafic que l'administrateur peut souhaiter interrompre au moyen des VACL. Ce flux circule du réseau interne vers les hôtes VPN. Pour ce faire, une VACL peut être dirigée vers le VLAN principal (41) et être combinée avec le précédent :

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

Test de la configuration

Nous envoyons un ping à l'hôte 10.1.1.1 à partir du routeur .193 (zundapp). Avant l'application de la VACL, le **ping** est positif.

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

Après l'application de la VACL sur le VLAN 41, le même **ping** échoue :

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

Cependant, nous pouvons encore envoyer un **ping** au routeur externe :

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

Informations connexes

- Configuration des listes de contrôle d'accès - Documentation du Catalyst 6000
- Support technique - Cisco Systems